Wireless Interference Analysis for Home IoT Security Vulnerability Detection

Alexander McDaid, Eoghan Furey, Kevin Curran

School of Computing,
Letterkenny Institute of Technology
Co. Donegal
Ireland
Email: eoghan.furey@lyit.ie

School of Computing, Engineering & Intelligent Systems, Faculty of Computing, Engineering & Built Environment
Ulster University, Northern Ireland
Email: kj.curran@ulster.ac.uk

Abstract - The integrity of wireless networks that make up the clear majority of IoT networks lack the inherent security of their wired counterparts. With the growth of the Internet of Things (IoT) and its pervasive nature in the modern home environment it has caused a spike in security concerns over how the network infrastructure handles, transmits and stores data. New wireless attacks such as KeySniffer and other attacks of this type cannot be tracked by traditional solutions. Therefore, this study investigates if wireless spectrum frequency monitoring using Interference analysis tools can aid in the monitoring of device signals within a home IoT network. This could be used enhance the security compliance guidelines set forth by OWASP and NIST for these network types and the devices associated. Active and passive network scanning tools are used to provide analysis of device vulnerability and as comparison for device discovery purposes. The work shows the advantages and disadvantages of this signal pattern testing technique compared to traditional network scanning methods. We demonstrate how RF spectrum analysis is an effective way of monitoring network traffic over the air waves but also possesses limitations in that knowledge is needed to decipher these patterns. We demonstrate alternative methods of interference analysis detection.

Keywords: Network Security, Wireless Security, Hacking, Internet of Things

1. Introduction

Wi-Fi and other communication technologies such as Bluetooth have existed for more than two decades and the volume of devices that utilise these technologies have exploded in recent years with a nearly 100% adoption rate. The term The Internet of Things (IoT) is commonly used to name a set of objects (or things) that are directly connected to the Internet via communication protocols such as Wi-Fi (802.11), Bluetooth and numerous other communication protocols. These networks consist of devices known as “Things” which can be constrained by hardware shortcomings that reduce their security effectiveness. Objects in the IoT are controlled via microcontrollers that are constrained in computational power, memory resources and power restrictions. These restrictions limit the devices from being able to utilise the same protocols that are used by higher powered computers like Transmission Control Protocol (TCP) and HyperText Transfer Protocol (HTTP) or modern encryption standards which are too resource consuming to be used on these highly constrained devices. A recent study conducted by HP Fortify on Demand research concluded that 70% of Internet of Things devices on the market are vulnerable to attack [1]. The Internet of Things is a phenomenon that is growing rapidly and is expected to include 50 billion devices connected to the internet by the year 2020 according to industry experts such as Michael Dell founder of Dell Inc. [2]. With this growth and the security constraints imposed on these devices by hardware shortcomings and security misconfigurations, it is predicted by Gartner Research that 20% of the overall security budget of major corporations will be spent trying to secure these devices [3]. Applications for this technology include agriculture, manufacturing, power distribution, to smart homes, healthcare, and beyond. All these sensory devices are connected to larger infrastructure produce an extraordinary amount of data. This technology advance acknowledges the reality that human society is moving towards ‘smart’ and ‘smarter’ systems. The rapid advances in computer science, software engineering, systems engineering, networking, sensing, communication, and artificial intelligence are converging [4].

With the rise of IoT networks in recent times and their expected exponential growth in the next five to ten years a way to effectively secure them will be of paramount importance [2]. There are few home or business owners that fully understand and recognise how their network exists and interacts with its surroundings and the threats that arise with the constant change in the number and type of devices that connect and disconnect on their networks. This shows the need for a better way to protect these IoT networks which is why the U.S. Federal Trade Commission (FTC) announced the launch of a contest that aims to find solutions for securing the Internet of Things (IoT) devices deployed in consumers' homes [5]. The FTC said the tool can be a physical device installed on the user's home network, an app, a cloud-based service, or a dashboard. The requirement is that the tool addresses vulnerabilities caused by outdated software, but it can also include other security features, such as ones designed to mitigate the risk of hardcoded or weak passwords.

With the rapid rise of the IoT phenomenon and the introduction of these poorly secured devices onto the network infrastructure have brought with them an avalanche of security concerns that consumers have about this encroachment into the home. These vulnerabilities have been well documented by the OWASP Internet of Things Project [6]. The vulnerabilities highlighted by this project have been exploited in some recent high-profile attacks. These Direct Denial of Service (DDoS) attacks are nothing new but because of the prevalence of these unsecured devices with high bandwidth capacity these attacks have become devastating against their targets. This form of attack has been levied against some high-profile targets such as Dyn Domain Name Server (DNS) Service [7]. Dyn which services a large portion of the DNS service in the United States was put under intense attack using this DDoS form of attack that utilised many thousands possibly hundreds of thousands of these IoT devices under the control of the Mirai malware. This malware was able to infect these devices to harness them as a huge botnet able to inundate the Dyn Servers with a huge amount of traffic that was able to knock out their service [7]. This attack has also been successful in knocking out the website of well-known security investigator Brian Krebs utilising the same malware to produce an attack that produced 620 Gbps of traffic against his website which was stated as a record amount of traffic for a Denial of Service attack according to Akamai security engineers [8]. Akamai have released a threat advisory explaining how to exploit IoT devices for launching mass-scale attack campaigns against a target and how to protect against this exploitation [9].

We therefore aim to investigate the effectiveness of using a set of professional tools that are designed to detect wireless interferences and to fix problems in a network environment. As a result, the objectives of the proposed research are:

- To investigate if a wireless interference and site survey planning toolset can be used as a preliminary scanning technique to detect network vulnerabilities before using network scanning methods.
- Can this technique be used as a component of an Intrusion Detection System (IDS) to detect and record potential malicious signals transmitted on the network that would not be seen by traditional IDS or scanning applications?
- To investigate if these techniques would be an effective addition to strength in depth layered IoT security architecture.

We investigate signals transmitted within the 2.4 and 5 GHz ISM frequency bands as these bands are the most commonly used communications bands in the home or business network environment.

2. Wireless Networks

There are numerous communication standards being used in the Internet of Things (IoT) at present such as Wi-Fi and Bluetooth which are available in every smartphone. There are also several other communication protocols being used by devices in the IoT domain such as Near-Field Communication (NFC), Mobile Communications (Cellular) and Radio Frequency Identification (RFID) which are not as widespread but have their own pros and cons associated with them. It is likely that the winner of these standards will be one that is available in most of the devices and phones. Today most smartphones have Bluetooth and Wi-Fi. However, NFC is increasingly being implemented in new phones and has its own pros and cons. There is no proposed unified standard communication protocol that these devices communicate on a network with. When there are several different communications protocols that devices can use to comprise an IoT network increases the attack surface of the network. This in turn increases the amount of security vulnerabilities an attacker can exploit. With multiple communications protocols being utilised on a network infrastructure this heterogeneous nature makes securing the network a harder prospect whereas if the network only utilised one communication protocol then the attack surface would be significantly reduced due to a reduced amount of vulnerabilities associated with other protocols.

2.1 Wi-Fi

Wi-Fi is a technology for wireless local area networking with devices which utilizes radio frequency technology (RF) based on the IEEE 802.11 standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term to Wi-Fi Certified products that successfully complete interoperability certification testing. The Wi-Fi Alliance formally known as Wireless Ethernet Compatibility Alliance (WECA) was founded in 1999, several companies came together to form a global non-profit association with the goal of promoting a new wireless networking technology. In 2000, the group adopted the term Wi-Fi as their trademark name for the IEEE 802.11 standard [10]. Wi-Fi is a Wireless Local Area Network (WLAN) that utilizes the IEEE 802.11 standard through 2.4GHz and 5GHz ISM frequencies. Wi-Fi provides Internet access to devices that are within the range of a wireless access point [11]. Wi-Fi is an excellent choice of communication protocol for wireless local area networks due to its universal adoption by all modern devices. The 802.11 standard is also well maintained and protected and the technology is prevalent and affordable. This makes Wi-Fi a useful technology for many Internet of Things connections but is not recommended for battery-powered constrained devices due to its relatively high-power consumption and the instability and inconsistency of signal coverage. Wi-Fi is aimed at use within unlicensed spectrum. This enables users to access the radio spectrum without the need for the regulations and restrictions that might be applicable elsewhere. The downside is that this spectrum is also shared by many other users and as a result the system must be resilient to interference. There are several unlicensed spectrum bands in a variety of areas of the radio spectrum. Often these are referred to as ISM bands - Industrial, Scientific and Medical, and they carry everything from microwave ovens to radio communications. Many of these bands, including the two used for Wi-Fi are global allocations, although local restrictions may apply for some aspects of their use [12]. The main bands used for carrying Wi-Fi are those in Tables 1 and 2:

Channel #	Lower Frequency MHz	Center Frequency MHz	Upper Frequency MHz
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Table 1: 2.4 GHz Wi-Fi Channel Frequencies Range

Channel Numbers	Frequency MHz
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
149	5745
153	5765
157	5785
161	5805
165	5825

Table 2: 5 GHz Wi-Fi Channel Frequency Range

There are fourteen channels defined for use by Wi-Fi 802.11 for the 2.4 GHz ISM band as seen in the Table 1. Table 2 shows the channels available in the 5 GHz ISM band. Not all the channels are allowed in all countries: 11 are allowed by the Federal Communication Commission (FCC) and used in what is often termed the North American domain, and 13 are allowed in Europe where channels have been defined by ETSI. The Wi-Fi channels are spaced 5 MHz apart with the exception of a 12 MHz spacing between the last two channels. The 802.11 WLAN standards specify a bandwidth of 22 MHz and channels are on a 5 MHz incremental step. Often nominal figures for the channel bandwidth of 20 MHz are often given. The 20 / 22 MHz bandwidth and channel separation

of 5 MHz means that adjacent channels overlap and signals on adjacent channels will interfere with each other [12]. The channels used for Wi-Fi are separated by 5 MHz apart from the final channel but have a bandwidth of 22 MHz which leads to an overlap of channels with a maximum of three non-overlapping channels 1, 6, and 1.

2.1.1 Wi-Fi Security Vulnerabilities

This explosive growth in wireless network technology along with the rapid evolution of the internet has seen an abundance of security threats emerge in recent years [13, 14]. The evolution and rapid adoption of mobile devices such as Tablet PC's, laptops and smart phones and a near 100% connection rate to a Wi-Fi infrastructure. The new mobile devices are given with more convenient functions and better portability than traditional PCs. These new features have brought Wi-Fi and mobile devices into people's daily lives [15]. The pervasive nature of these devices in daily life has led to numerous security issues that are associated with Wi-Fi technology. Common Wi-Fi security vulnerabilities can be seen in a summary in Table 3.

Table 3: Wi-Fi Security Vulnerabilities

Vulnerability Name	Vulnerability Description
Default configurations	Default configurations are especially dangerous when left as-is simply because the medium (open air) used is available to everyone within a certain geographic radius. Default configurations really depend on the product and the vendor involved as the default credentials are easily obtainable on the internet.
Rogue Access Points	A rogue access point is a wireless access point that is illicitly placed within, or on the edges of, a Wi-Fi network posing as a legitimate AP [16].
Encryption Weakness	Weak encryption standards example WEP the encryption algorithm RC4 used in WEP is flawed and encryption keys can be recovered through cryptanalysis [16]. Thus more secure encryption such as WPA2 should be adopted
Man in the Middle Attack (MITM)	A Man-in-the-Middle attack can be used to read the private data from a session or to modify them, thus, breaking the confidentiality and integrity of the data. This attack occurs when a malicious user inserts himself between two parties in a communication and impersonates both sides of the exchange. The attacker then intercepts, sends and receives data meant for either user which breaks data confidentiality [16].
Denial-of-Service (DoS)	A denial-of-service attack where a perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet [16]. This is accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.
Replay Attack	This attack uses the legitimate authentication sessions to access the WLAN. The attacker first captures the authentication of a session. The attacker replays authenticated sessions to gain access to the network without altering or interfering with the original session or sessions [16].
Session Hijacking	An attacker takes an authorized and authenticated session away from the legitimate user of the network. The user has no idea that the session has been taken over by the attacker. This attack occurs in real-time [16].

2.2 Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz. The Bluetooth channels are spaced 1MHz apart, beginning at 2402MHz and ending at 2480MHz utilizing 79 individual Bluetooth channels. This uses a similar frequency range to Wi-Fi and other potential interfering devices thus Bluetooth utilizes a Frequency Hopping Spread Spectrum (FHSS) mechanism [17]. Bluetooth uses this technique to communicate by hopping frequency rapidly using a pseudo random pattern across the range to combat interference from devices communicating over the same frequency range. The objective of Bluetooth was to replace cables with short range wireless communication due to its limited range this technology has found use for several peripheral devices such as keyboards, mice, headsets, radios and hands-free kits [17]. There have been numerous changes and upgrades that have been released over the years that have increased data rate throughput, increased security and lowered power consumption. The introduction of Bluetooth Low Energy 4.0 (BLE) in 2010 offered a number of advantages over previous iterations of the Bluetooth standard this includes low cost, low energy consumption, security enhancements and small size making this ideal for IoT device integration [17].

2.2.1 Bluetooth Security Vulnerabilities

Due to implementation of millions and millions of Bluetooth devices in use, malicious security violations are now common events and are expected to increase soon. With the increased usage of Bluetooth devices this makes security concerns even more alarming [18]. See Table 4 for a list of common Bluetooth vulnerabilities.

Table 4. Bluetooth Security Vulnerabilities

Vulnerability Name	Vulnerability Description
Bluejacking	Bluejacking is the process of sending unsolicited messages to Bluetooth enabled devices. It is a passive attack in which victim is flooded with anonymous messages. This attack can easily be carried out in a crowded area where a number of unsuspecting victims are easily found. This attack uses the —obex push attack vulnerability. Many of the Nokia, Sony and Motorola mobile phones have been targeted with this attack [18].
Bluebugging	It uses the Address Translation (AT) commands available in GSM phones. An attacker exploits these commands to steal personal information like phonebook contacts and messages. Even phone calls can be initiated. Unwanted messages, viruses, worms can be sent from victim device to any other device [18].
Backdoor attack	This is when a hacker establishes trusted relationship with a handset, but then ensuring that it no longer appears in the target's registry of paired devices. This connection is granting him access not only to the data on your phone but also allowing him to use WAP/GPRS services [18].
DoS attack	BD_ADDR duplication attack: The bug duplicates the BD_ADDR of the target device. When any Bluetooth device tries to make a connection with the target device, either the target device or both devices will respond and jam each other. SCO/eSCO attack: It is based on a real-time two-way voice. It reserves a great deal of a Bluetooth Piconet's attention so that the legitimate Piconet devices are not allowed to get the service within a reasonable period of time L2CAP Guaranteed Service attack: An attacker requests the highest possible data rate or the smallest possible latency from the target device so that all other connections are refused, and the throughput is reserved for the attacker [18].
Pin cracking attack	This is most important security vulnerability in the Bluetooth technology. Security of Bluetooth communication is totally dependent on the user defined shared secret i.e. pin number [18].
Car Whispering	This involves the use of software that allows hackers to send and receive audio to and from a Bluetooth enabled car stereo system [12].

While Table 4 contains several common vulnerabilities associated with previous iterations of the Bluetooth standard the adoption of Bluetooth 4.0 (BLE) has rendered a number of these attack vectors obsolete. BLE has enhanced security rendering some these attack scenarios such as Bluejacking obsolete but has reintroduced other vulnerabilities such as Denial of Service (DoS) attacks back into the research community's mind. These DoS attacks have evolved into Denial of Sleep attacks that attempt to drain these devices of their limited power resources. By denying the devices the ability to enter their idle mode these constrained devices will eventually become drained of power thus perpetrating a Denial of Service attack [19].

2.3 ZigBee

Radio frequency communications are probably the easiest form of communications between devices. Protocols like ZigBee or ZWave use a low-power RF radio embedded or retrofitted into electronic devices and systems. Z-Wave has a range of approximately 100 ft. (30 m). The radio frequency band used is specific to its country. For example, Europe has an 868.42 MHz SRD Band, a 900 MHz ISM or 908.42 MHz band (United States), a 916 MHz in Israel, 919.82 MHz in Hong Kong, 921.42 MHz in the regions of Australia/New Zealand) and 865.2 MHz in India [11]. ZigBee is based on the IEEE 802.15.4 standard. However, its low power consumption limits transmission distances to a range of 10 to 100 meters. Radio frequency technology is not used by smartphones and without a central hub to connect the RF devices to the internet, the devices cannot be connected. Uses for this technology because of its inherent limitations would be wireless light switches, electrical meters and other devices that require short-range low data traffic transmission.

2.3.1 ZigBee Security Vulnerabilities

The primary issue is that if manufactures of ZigBee devices use the default settings to exchange secure keys among other devices in the ZigBee network, it introduces a weakness. It is the equivalent of manufacturers using "password" as their password for exchanging these keys. Another manufacturing problem is using low-end radios that aren't tamper proof for the "dumb" devices in the network such as sensors. The popular wireless mesh networking protocol used in many connected home devices including the Philips Hue light bulbs has been shown to be vulnerable to intrusion. The way that the ZigBee wireless protocol authenticates devices in its mesh network leaves it open to attack, despite the protocol's use of high quality security [20]. A summary of common Zigbee security vulnerabilities can be found in Table 5.

Table 5. Summary of ZigBee Vulnerabilities [20]

Attack Type	Attack Description
Physical Attack	Radios residing on the network employ a hard-coded encryption key loaded in the RAM memory once the device is powered. An attacker can set up special serial interfaces on the ZigBee device in order to intercept the encryption keys moved from flash to RAM during power up.
Key Attack	Remote attacks aiming to snatch encryption keys are possible due to Over the Air (OTA) key delivery and pre-shared keying inherent to ZigBee. Security can be circumvented with a device that mimics a ZigBee node and picks up the transmission exchanged among internal devices; these packets can be analysed or decrypted to recover the key.
Replay & Injection Attack	Replay or Injection goal is to dupe ZigBee devices into executing unauthorized actions. ZigBee units are particularly vulnerable to these attacks, since they are equipped with a lightweight design of the protocol with weak replay protection. Captured packets from ZigBee nodes are sent back in a replay attack scenario to make it look that they come from the originating node.

2.4 Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is the wireless use of electromagnetic fields to identify objects. Usually you would install an active reader, or reading tags that contain stored information mostly authentication replies. This is known as an Active Reader Passive Tag (ARPT) system. Short range RFID is about 10cm, but long range can go up to 200m [11]. An Active Reader Active Tag (ARAT) system uses active tags awoken with an interrogator signal from the active reader. Bands RFID runs on: 120–150 kHz (10cm), 3.56 MHz (10cm-1m), 433 MHz (1-100m), 865-868 MHz (Europe), 902-928 MHz (North America) (1-12m) [11]. The Advantages of this technology are that it is a well-established technology that is widely used is such environments such as animal tagging, building access through keycards and can also be utilized for inventory tracking in manufacturing. The disadvantages of this technology are ongoing worries over the security concerns of this form of communication and its compatibility with other technologies [21]. RFID is a technology that in recent years with the introduction of Near Field Communication (NFC) on most modern mobile devices looks to becoming obsolete.

2.4.1 RFID Security Vulnerabilities

The use of Radio Frequency Identification (RFID) technology can be observed in several areas of industry. Companies and government agencies have implemented RFID solutions to make their inventory control systems more efficient and to obtained access through keycard technology. In spite of the benefits that RFID can provide to industry, there are glaring security concerns that come with its use [22]. A summary of common RFID vulnerabilities can be seen in Table 6.

Table 6. Summary of RFID Vulnerabilities

Attack Type	Attack Description
RFID Spoofing	The process of unauthorized capturing of RFID tag information, including its unique tag ID (TID), and the retransmitting of this information to a reader thereby fooling it into believing that the data is coming from a legitimate transponder [23].
Tag Cloning	When RFID spoofing is done coupled with replicating the original form factor of the tag to give an identical product, the RFID tag is said to have been cloned. RFID cloning is also referred to as a, relay attack [23].
Side Channel Attacks	Rouge RFID readers can sniff RF communications between authorized tags and readers and might use confidential information [23].

3. Wireless Security

An intrusion detection system (IDS) monitors network traffic for suspicious activity and alerts the network administrator or is collected centrally using a Security Information and Event Management (SIEM) system. There are IDS that detect based on looking for specific signatures of known threats similar to the way antivirus software detects and protects against malware and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat a summary description of these types can be seen in table 8 [25].

Table 7: IDS Types

IDS Type	IDS Description
Network intrusion detection systems (NIDS)	Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic.
Host intrusion detection systems (HIDS)	Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected.
Signature Based	A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
Anomaly Based	An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous.
Passive IDS	A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.
Reactive IDS	A reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat.

Modern IDS solutions are well developed and usually comprise of a combination of several types of IDS bundled with an IPS solution and a firewall in an enterprise environment but in an IoT environment these heavy systems are not feasible on constrained networks. While modern IDS/IPS solutions are effective with detecting traffic coming into the network there are situations where these systems are ineffectual with detecting intrusive devices intruding on the network while not transmitting through a network connection. Several modern attack scenarios have been highlighted by security researchers such as Bastille Research Team that cannot be detected by an IDS solution. KeySniffer is a set of security vulnerabilities affecting non-Bluetooth wireless keyboards. The wireless keyboards susceptible to KeySniffer use unencrypted radio communication, enabling an attacker up to several hundred feet away to eavesdrop and record all the keystrokes typed by the victim. This means an attacker can see personal and private data such as credit card numbers, usernames, passwords, security question answers and other sensitive or private information all in clear text [26]. Another prominent vulnerability has been displayed by a security researcher for Red Balloon Security Ang Cui who set out to create intentional radio signals that could be used as a carrier to broadcast data to an attacker even in situations where networks were "air-gapped" from the outside world. The result of the work of his research team is Funtenna, a software exploit he demonstrated at Black Hat security conference that can turn a device with embedded computing power into a radio-based backchannel to broadcast data to an attacker without using Wi-Fi, Bluetooth, or other known (and monitored) wireless communications channels [27]. The only type of solution to this kind of security problem exists in expensive hardware and vulnerability detection software combinations. These systems are out of the reach of the common householder such as the AirMagnet system or the moderately priced Cisco Clean Air system that combines spectrum analysis inside the router package.

Another prominent vulnerability highlighted in recent times is the ability to determine keystrokes made through analysis of the Wi-Fi signal produced by the keystroke itself. We can categorise this technique into three categories; acoustic emission-based approaches, electromagnetic emission-based approaches, and vision-based approaches [28]. Acoustic emission-based approaches recognize keystrokes based on either the observation that different keys in a keyboard produce different typing sounds or the observation that the acoustic emanations from

different keys arrive in different surrounding at different times as the keys are located at different places on a keyboard. Vision based approaches recognizes keystrokes using vision technologies. These categories are not of interest to this study. Electromagnetic emission based approaches recognize keystrokes based on the observation that the electromagnetic emanations from the electrical circuit underneath different keys in a keyboard are different. Wi-Fi signals can be exploited to recognize keystrokes. Wi-Fi signals are pervasive in our daily life at home, offices, and especially in large venues such as shopping centres. While typing a certain key, the hands and fingers of a user move in a unique formation and direction and generate a unique pattern in the time-series of Channel State Information (CSI) values, which we call CSI-waveform, for that key. The keystrokes of each key introduce relative unique multi-path distortions in Wi-Fi signals and this uniqueness can be exploited to recognize keystrokes [28].

3.1 Security Guidelines and Compliance

The National Institute of Standards and Technology (NIST) routinely publish special publications of interest to the computer security industry. These publications cover guidelines on several different technologies within these networks not all of which are transferable but are useful for a defence in depth approach to network security.

1. **NIST Special Publication 800-183 - Networks of 'Things'**
   This document offers an underlying and foundational understanding of IoT based on the realization that IoT involves sensing, computing, communication, and actuation. The material presented here is generic to all distributed systems that employ IoT technologies [29]. This document relates to scalability concerns, heterogeneity concerns, temporal concerns, and elements with possible nefarious intent. The rapid advances in computer science, software engineering, systems engineering, networking, sensing, communication, and artificial intelligence are converging. The tethering factor is data. There is no formal, analytic, or even descriptive set of the building blocks that govern the operation, trustworthiness, and lifecycle of IoT. This document intends to address this concern and offers an underlying and foundational science to IoT based on a belief that IoT involves sensing, computing, communication, and actuation [4, 29].

2. **NIST Framework for Cyber-Physical Systems (Draft)**
   Although this document is currently in draft phase it contains information relevant to Cyber-Physical Systems (CPS) which are smart systems that include co-engineered interacting networks of physical and computational components. CPS and related systems including the Internet of Things, Industrial Internet, and more are widely recognized as having great potential to enable innovative applications and impact multiple economic sectors in the worldwide economy [29]. The CPS Framework when ready will be a guide that can be used when developing these large systems as well as being adapted to a smaller scale operation.

3. **NIST SP 800-121 (Revision 1) - Guide to Bluetooth Security**
   NIST's publication provides a 33 point checklist used in securing and maintaining Bluetooth piconets and the sensitive communications transmitted on a network [30]. This document can be used to help mitigate the myriad of vulnerabilities associated with Bluetooth devices which are susceptible to general wireless networking threats, such as denial of service (DoS) attacks, eavesdropping, man-in-the-middle (MITM) attacks, message modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized use of Bluetooth devices and other systems or networks to which the devices are connected [30].

4. **NIST Special Publication 800-94 Revision 1 Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) (2012)**
   Intrusion detection and prevention systems (IDPS) are focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. This publication describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them [31]. This document provides important advice about securing wireless communications within the network environment such as recommendations on sensor locations "wireless sensors should be deployed so that they monitor the Radio Frequency (RF) range of the

organization's Access Points (AP's) which includes both stationary and mobile components which can exist in an IoT network

5. **PCI-DSS 3.0**
   This provides guidance and installation suggestions for testing and/or deploying 802.11 Wireless Local Area Networks (WLAN) for organizations that require Payment Card Industry's Data Security Standard (PCI DSS) v1.2 compliance [33]. Compliance with these guidelines does not guarantee the security of sensitive data transmitted on the network and PCI Council recommends that official reviews of the organisation security stance should takes place periodically. The organisation should scan their entire network for potential vulnerabilities that might have not existed during the previous organisation wide security audit.

4. Evaluation

Securing modern networks require network monitoring, security auditing tools, antivirus software, IDS/IPS systems and firewalls. However, when an attacker uses wireless snooping techniques, current solutions have no way of tracking this activity so another method needs to be employed. Here we outline the test rig needed to track an attacker injecting data through RF signals to input his own commands to susceptible devices [26].

Devices used for testing included Samsung Galaxy S2, Amazon Kindle Fire HDX, Vu+ Duo, Samsung Smart TV (UE46C8000), Motorola Focus66-W Wi-Fi Home Video Camera, Microsoft Bluetooth Entertainment Keyboard 8000, Microsoft Bluetooth Laser Mouse 8000 and Fitbit Surge. The spectrum analyser (Ekahau) in conjunction with the Chanalyzer software from MetaGeek was installed and setup on a Lenovo Yoga Book as this equipment was decided to be an excellent choice to conduct testing due to its ease of use and its lightweight and compact form factor design. A walk through of the test area was performed to discover what devices are communicating over the network. Testing was completed in four steps as described in the following section.

Step 1 of testing involved attempting to identify individual devices powered up in isolation to ensure that there were no interfering signals to obtain the specific devices waveform signature. This test was conducted with a configuration of a Lenovo Yoga Book test laptop with Chanalyzer software in conjunction with the Ekahau Spectrum Analyser with the stock accompanied Omni-directional antenna. This test setup was used with the Omni-directional antenna to ensure there were no other interfering signals other than the one that was being tested for. Once a clear signal of the test device was established step 2 could proceed.

Step 2 of testing involved fitting a directional antenna to the Ekahau Spectrum Analyser this antenna is used to find a test device by isolating the device by their signal pattern and locating them via proximity due to their signal strength. This is accomplished with the help of the Chanalyzer software and its device finder feature. Once the test signal is isolated it would show the devices proximity to the testing apparatus by way of a real-time bar chart of signal strength that would show a strong signal strength when close and a weak signal strength when moving away from the devices signal.

Step 3 of testing involved powering up all the devices in the test list in specific locations throughout the test area in order to ascertain if a specific device could be isolated and found by walking through the test area over the cluttered noise of a busy network.

Step 4 involves performing testing on a large surrounding area and was performed to highlight how a wireless network interacts with its environment and to highlight just how far your wireless network can expand to the surrounding environment which can lead to security concerns. This test involved conducting a heat mapping of the wireless network area provided by the network infrastructure used during testing and the competing neighbouring wireless signals and environment that are factors surrounding it. The detailed information provided by Ekahau's Site Survey and Planning software and the wireless network adapter scanning USB dongle provided additional network information. The test route taken can be seen in figure 2 and was used by the equipment to calculate the network signal pattern and strength results.

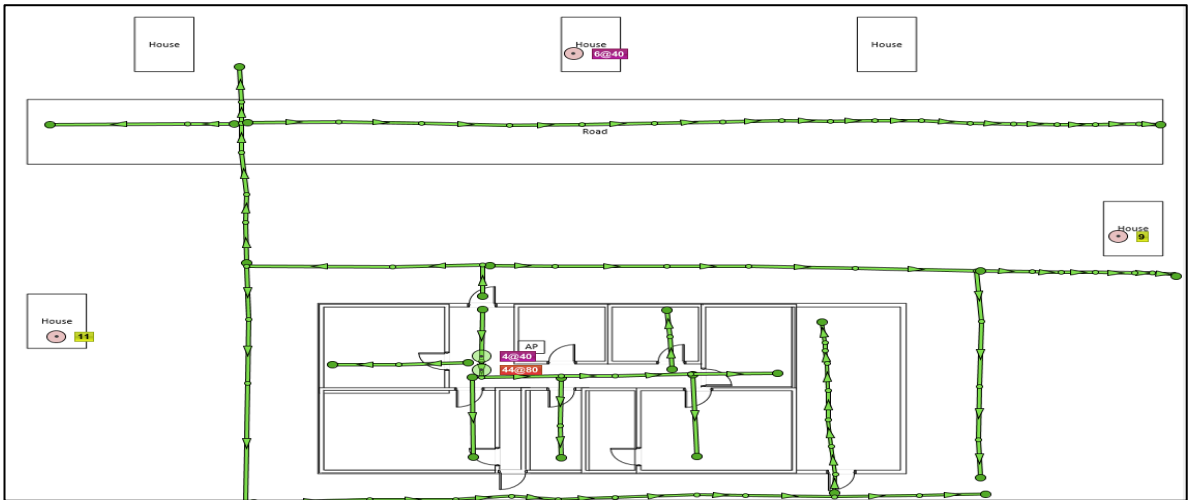

Figure 1: Network Range Test Walkthrough Route

Vulnerability analysis testing of the devices found by the RF spectrum scans conducted in the test area was conducted in order to provide additional vulnerability information. Network Scans were conducted using freeware network scanning tools for mobile devices and a powerful network scanner based on the Python scripting language called Nmap available on both the Windows and Linux operating platforms. Scanning tools included Nmap (Network Scanner), WiFi Network Analyser, NetGear Genie, Net Scan and Bluetooth Scanner.

4.1 Initial RF Signal Scan Results

The initial tests were accomplished at this stage by scanning the test devices in isolation to obtain their specific signal pattern. We can see from the signal pattern observable from the density view in figure 3 that the device transmitting impacts all the channels in the 2.4 GHz band. This device is known to be a Hinari Microwave which operates in the 2.4 GHz band across all channels. This signal pattern is seen in the amplitude peak on channel 11.

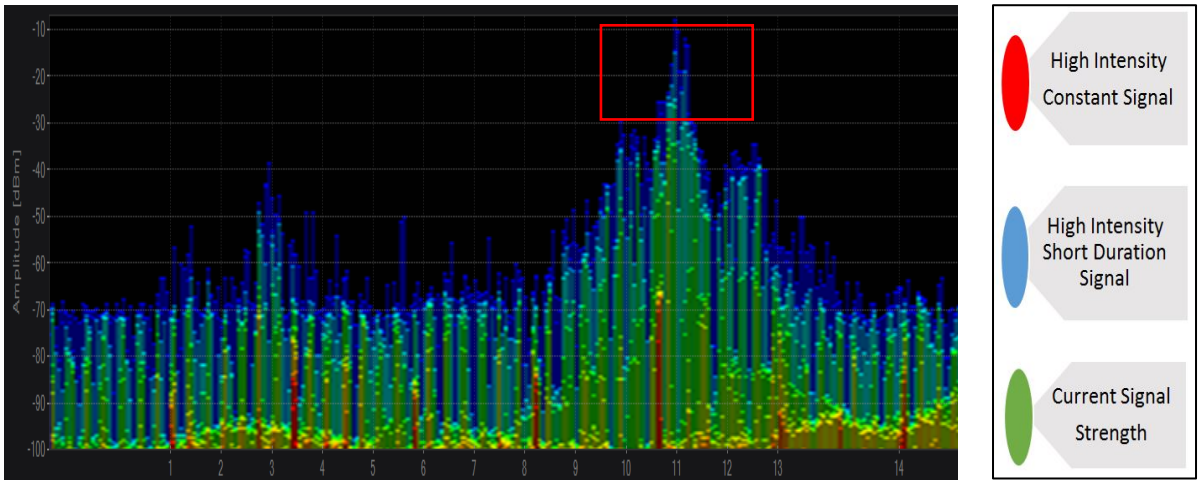

Figure 2: Microwave Common Network Interferer

This would degrade the signal that any other device transmitting on channel 11 due to its high intensity. This signal pattern could be used to perpetrate a Denial of Service attack by flooding the airwaves but is unlikely to occur as Microwave signals are known to occur in the network environment but for only a short duration making this an infrequent signal nuisance. Although this signal interference is not a traditional security threat to the network the signal pattern impact could be used to mask other malicious signals that would become harder to isolate because of this signal noise.

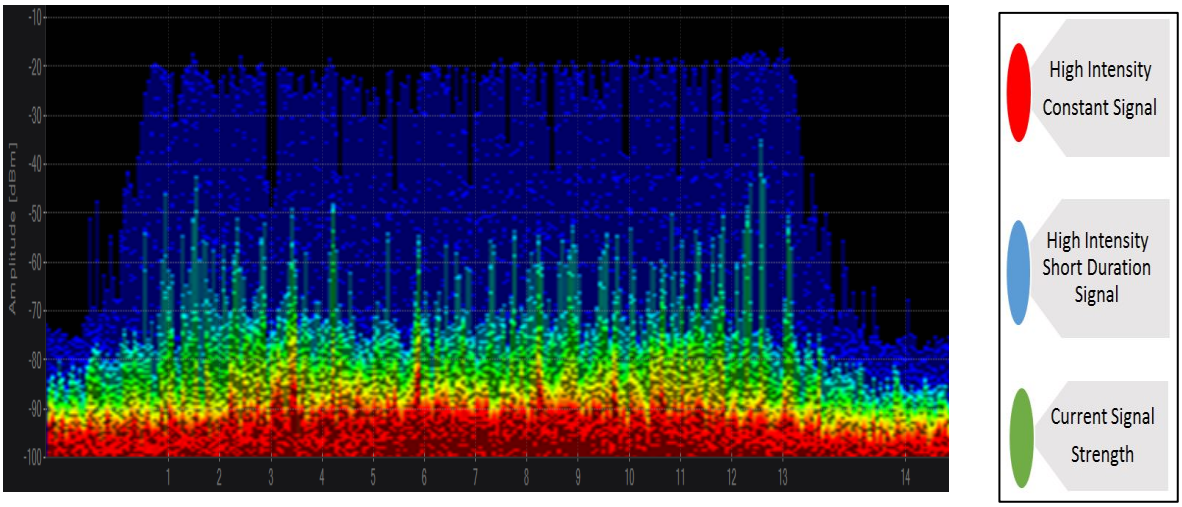

Figure 3: RF A/V Baby Monitor Common Network Interferer

We can again see from the signal pattern observable from the density view in figure 4 that shows the device transmitting impacts the entire 2.4 GHz band across all channels. This device is known to be a Motorola MBP33 Baby Monitor that transmits an RF video signal over 2.4. This signal is a known signal interferer and produces a high intensity signal across the test frequency band like the Microwave signal. Unlike that signal the transmission amplitude intensity is not as strong but is constant over a longer period producing significant interference to any devices transmitting within its vicinity. This signal again is not a traditional threat to the IoT network but like the Microwave signal previously discussed could be used to perpetrate a DoS attack if several of these devices where used throughout the test environment.

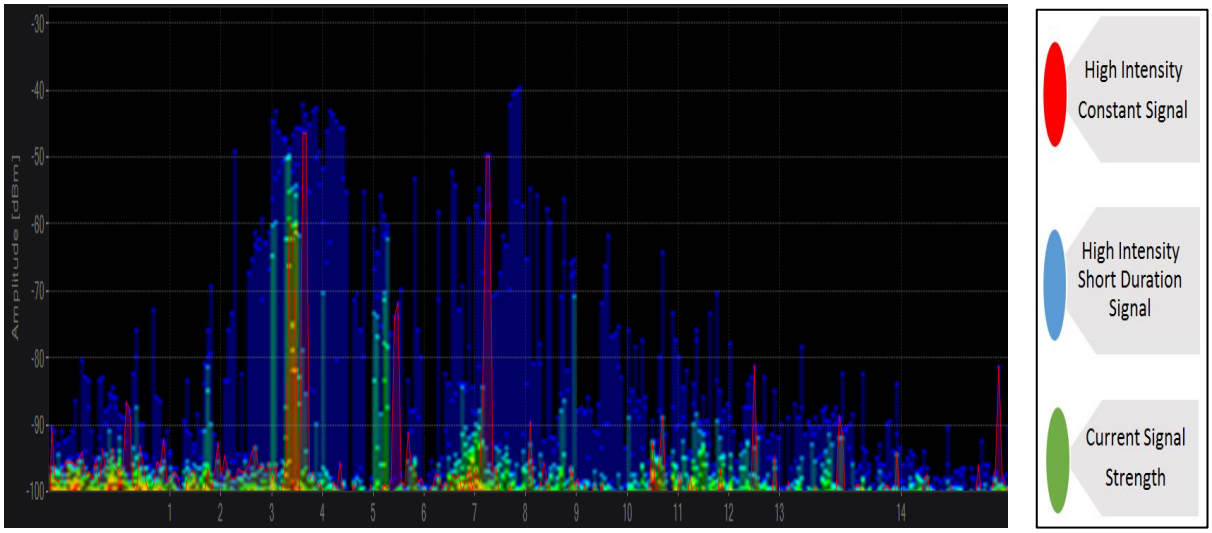

Figure 4: Cordless Phone Common Network Interferer

The Panasonic KX-TG7321E cordless phone can be observed in figure 5 demonstrating its typical frequency hopping nature while causing signal interference throughout the entire 2.4 GHz frequency band as shown by the red spikes. These cordless phones were designed to eliminate the threat of significant signal interference due to the nature of the signal produced by these devices that mimic the same frequency hopping nature of the Bluetooth protocol. These devices can impact all of the channels within the 2.4 GHz test band but because they hop channel so frequently they have little impact on the network from a signal degradation standpoint.

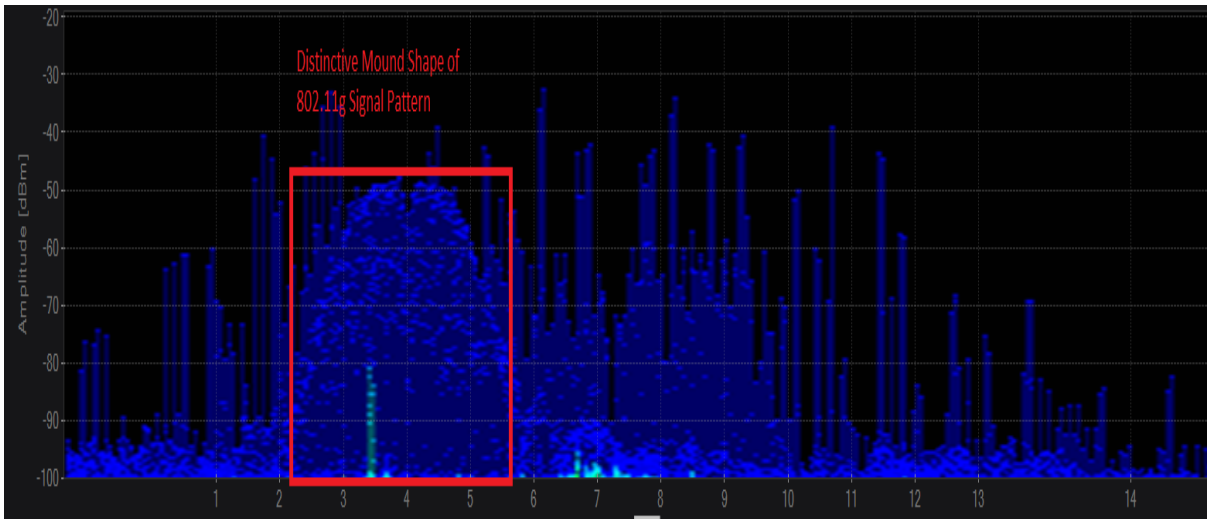

Figure 5: Vu+ Duo Streaming Set Top Box

The signal observed in the frequency scan in figure 6 is an 802.11g transmission attributed to the Vu+ Duo Set Top Box due to its wireless adapter being a Belkin 802.11g adapter with a 54mb data rate. This type of device is becoming more prevalent in the modern home IoT network due to their use as a media streamer. These devices use a simple Linux based operating system that is fully connected to the network environment and can stream media from the internet or private servers. These devices could also contain numerous security vulnerabilities due to the simplicity of their design and limit of their resources. Further analysis of this device at the network level will have to be performed to determine if this device has any known security vulnerabilities.

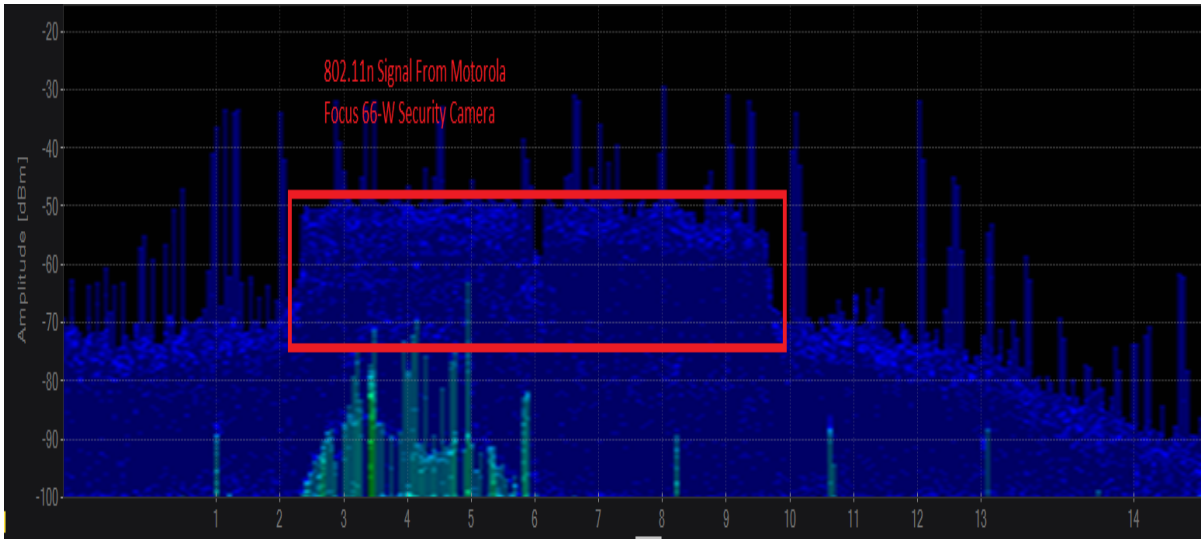

Figure 6: Motorola Focus66-W Security Camera

Figure 7 shows the pattern attributed to an 802.11n signal the flat table like mountain with a crevice in the middle which is what the communication standard used by the Motorola Focus66-W security camera. This device and many like it have been the talk of the research community for several years due to their lack of adequate security which has rendered them open to the masses while existing in a user's home. These devices have also come under increased scrutiny in the past year as they have become a target for several malware bots that have utilised their high data throughput to produce several outages in key parts of the internet's infrastructure such as the Dyn servers. These pieces of malware previously discussed in this research such as the Mirai malware can turn these devices into powerful attack systems if enough of them are combined to create massive DDoS attacks. We also mapped the patterns for the Galaxy S2, Microsoft 8000 Series Bluetooth Keyboard & Mouse Wireless Pioneer MVH-X580DAB Bluetooth Radio.

4.2 Proximity Location Finding of Devices

Initial RF scans of the test devices that were accomplished in isolation were successful in that each device tested had a recognisable RF pattern. These initial scans show this scanning practice can be a valuable testing technique to uncover what devices and communications protocols and standards are transmitting on the home IoT network. Although these tests are encouraging during this testing phase in its ability to uncover transmitting devices on the network further analysis of these devices will have to be conducted to ascertain if they contain any security vulnerabilities. This analysis will be performed by traditional network scanning methods.

The following tests were accomplished using the device finder functionality of the Chanalyzer software. This requires the test devices to be isolated in the amplitude graphs and using the device finder function seen in figure 8. The stronger the signal observed on the left side of the graph highlights the closer the offending device is and the lower the signal seen on the right side of the graph the further away you are from the device you are. This testing technique will allow a tester to find any device within an area as long as they can isolate the devices transmission spectrum pattern.

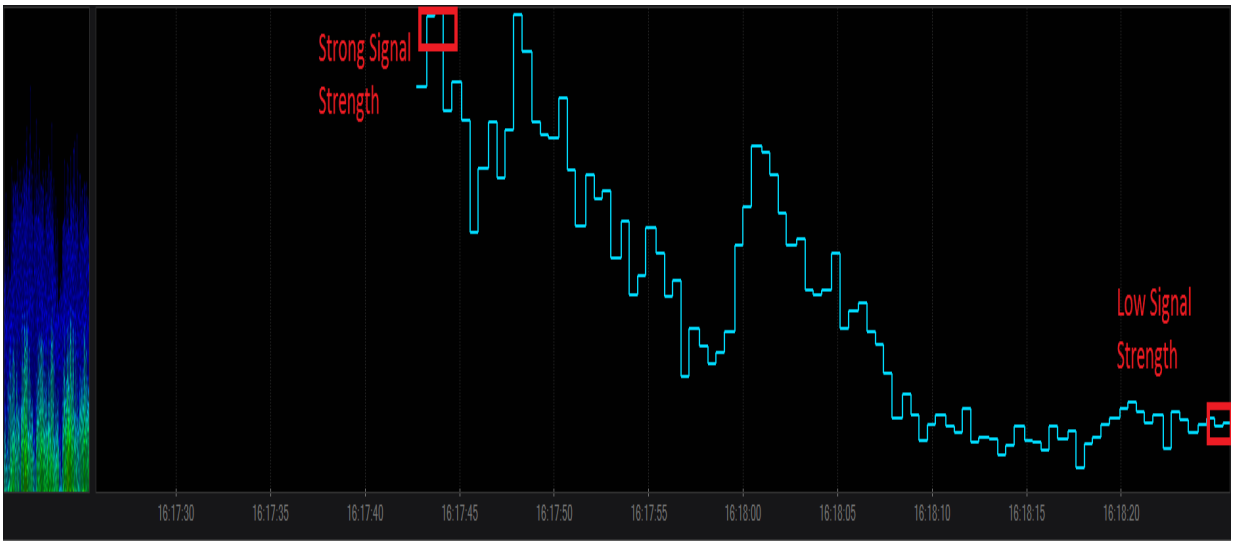

Figure 7: Device Finder Proximity Location

The proximity location testing provided the expected results for the devices with a clear signal pattern such as the devices transmitting with the Wi-Fi standards. This testing technique was effective in tracking these devices signals to their physical location. While this testing technique was effective in finding the test devices using the Wi-Fi standard it was less effective in locating the Bluetooth devices. This was due to the transient nature of the Bluetooth signals making it harder to get a lock on their signals to isolate in the device finder and this functionality could use some refinement in the future.

A noisy location reconnaissance test was conducted by placing test devices throughout the test area and performing a walkthrough to find and identify these devices transmitting on a busy network. The test area and location of devices can be observed in figure 9. By isolating a specific devices spectrum pattern and using the device finder function of Chanalyzer the device can be tracked down to a specific location. This technique has its problems as without a clear signal pattern or a signal pattern of similar type within an area of clustered devices might make the test less effective. Although this would still lead you to that area and further investigation could be employed. The size of the test bed was 8 meters by 14 meters.

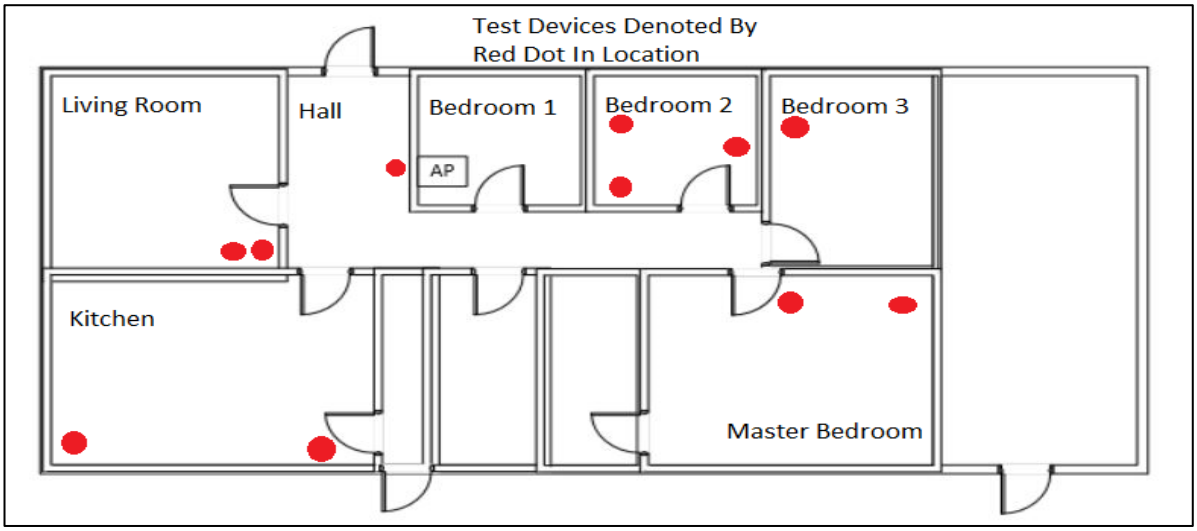

Figure 8: Device Identification Walkthrough Test Area

In figure 10 we can see the problems that would be encountered in a noisy environment but we can still see distinctive signal patterns within the signal environment. While the test environment is cluttered, distinct signal patterns can still be observed through the noisy environment as shown in figure 10. The device signals observed are the Motorola Focus66-W Security Camera, Samsung Galaxy s2, Panasonic KX-TG7321E cordless phone and the Hinari Microwave Oven. These devices can be observed from the test environment where the devices were powered on to create a loud signal pattern. This was done to ascertain whether this testing technique could be adapted to find specific devices within a noisy signal environment.

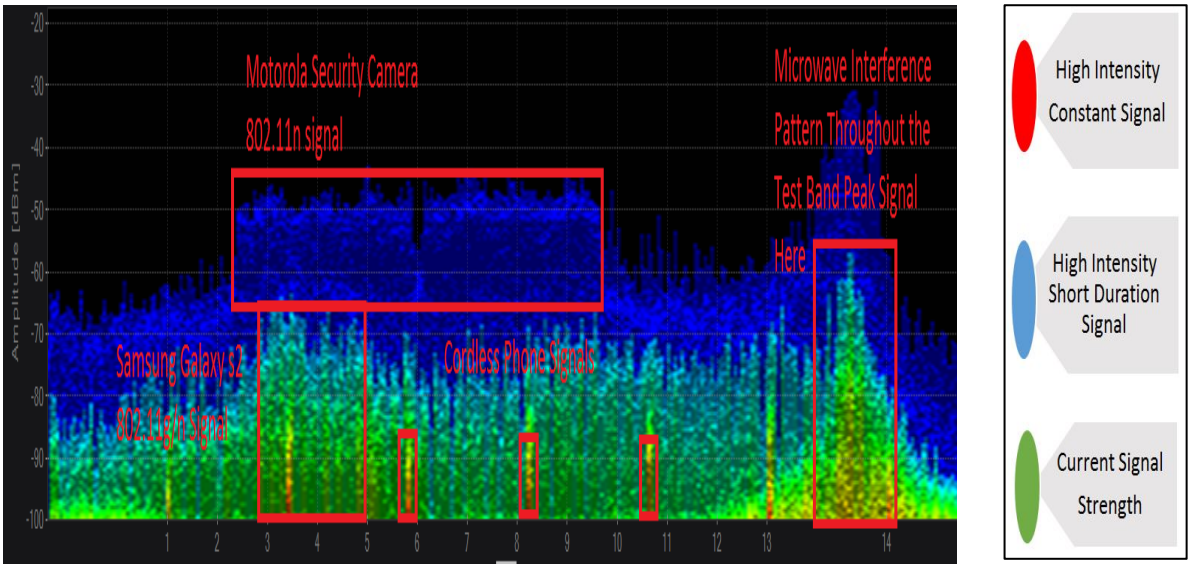

Figure 9: Several Test Devices Transmitting in Proximity

The findings observed were that in a noisy test environment, devices with a distinct transmission pattern that was loud enough could be found through the noisy environment. While this was effective in finding devices like the security camera observed in figure 10. it was less effective in finding devices that transmit at a relatively low amplitude such as the cordless phone seen the only reason that this device was able to be found was due to previous tests accomplished in isolation and because this device was known to be in the test environment. From this test it can be concluded that further work could be done to refine this software to be able to recognise these devices from their signal pattern, frequency range and signal amplitude output.

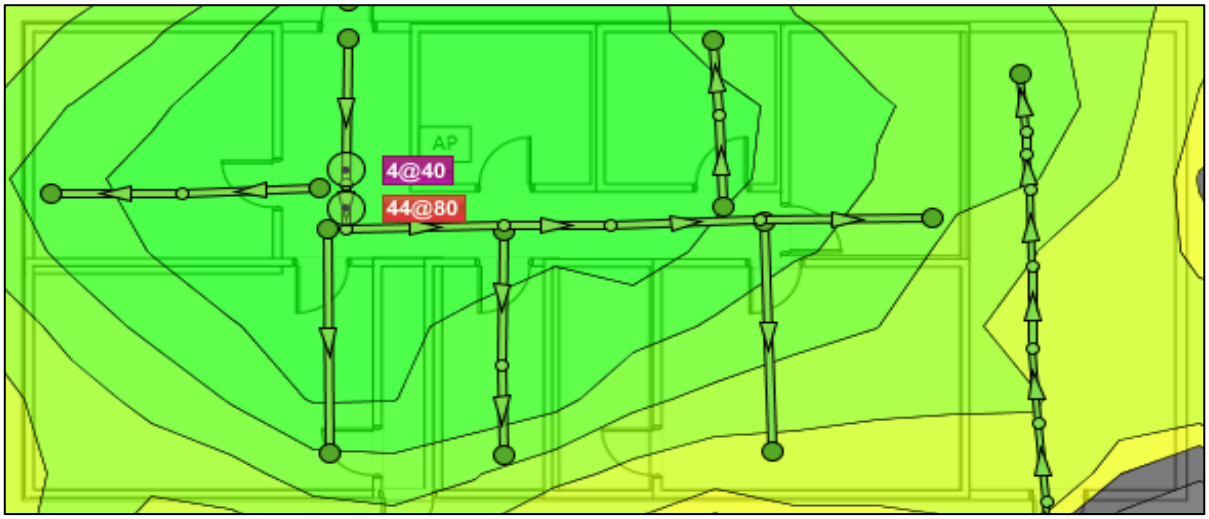

Figure 10: Indoor Test Area Heat Map of Signal Strength

Heat mapping of the environment was conducted in two stages these stages were separated to the indoor and outdoor stages of this test phase. The indoor testing shown in figure 11 shows that the signal strength coverage of the wireless network covers the entire test area with a -60dBi or greater signal strength. This provides the test devices within the test area the required data rate to operate to their potential. We can observe from figure 11 that two AP's are present within the test area these wireless networks are the 2.4 GHz network transmitting on channel 4 and the 5 GHz network transmitting on channel 44 by the NetGear router hosting the IoT network.

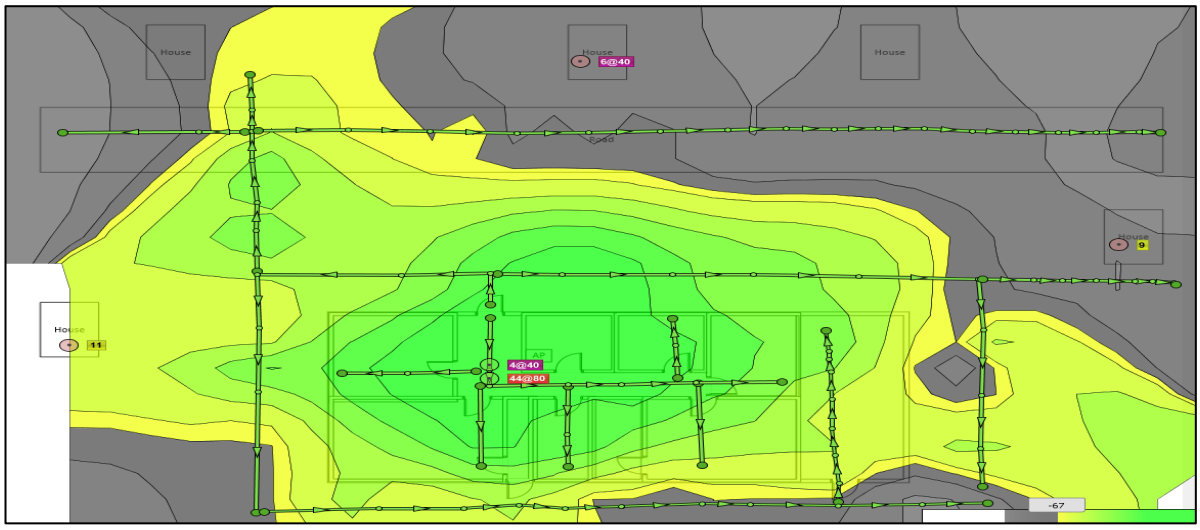

Figure 11: Indoor/Outdoor Heat Map of Signal Strength

The outdoor testing in figure 12 shows the extent of coverage of the wireless network in the surrounding environment. This gives the author an idea of the coverage area of the AP that exists outside of the expected test area. We can observe that two AP's are present within the test area. These wireless networks are the 2.4 GHz network transmitting on channel 4 and the 5 GHz network transmitting on channel 44 by the NetGear router hosting the IoT network. Other AP's can also be observed in this test from the surrounding houses in the test area and the channels they are transmitting on. Figure 13 displays the signal strength according to its corresponding dBm strength.

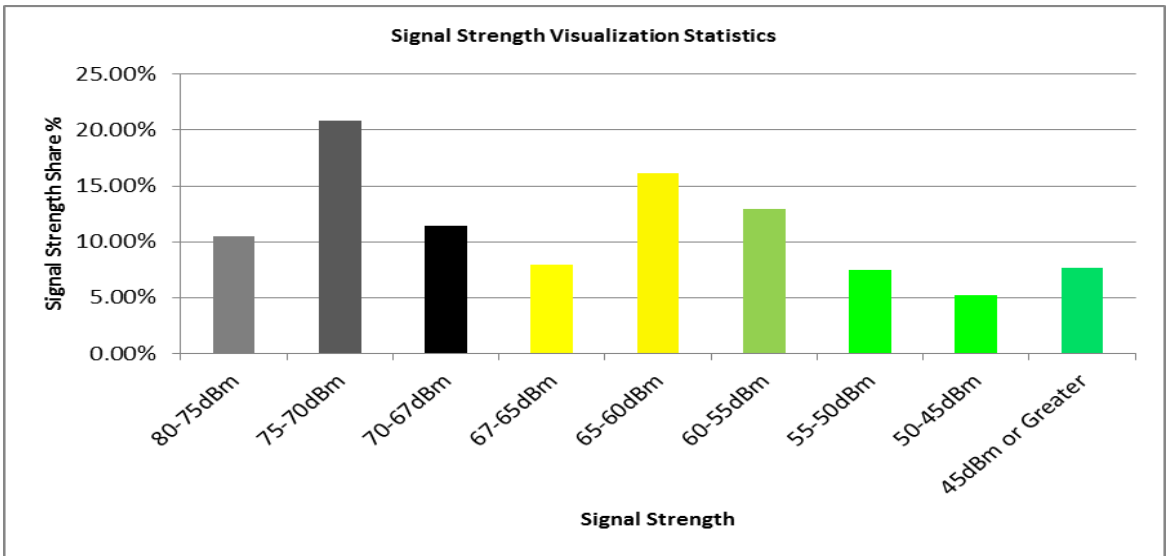

Figure 12: Signal Strength of Network Environment

This site surveying software was effective in discovering the AP's transmitting within the test area. 7 access points were found to be transmitting within the test range of the site survey's USB network adapter. This was particularly impressive as two of the AP's detected were significantly outside of the test area. Not only did the site survey equipment find the transmitting AP's within the area it was able to detect the MAC address and the encryption standards used to secure them. This information would be of interest to an attacker who could use the information to make a map of all the access points in an area using the same testing techniques employed here to get a complete picture of his environment. This equipment is effective as an initial site scanning tool but lacks the ability to detect individual devices within the test networks. The findings observed from this testing phase were that the Ekahau Site Survey software was effective at visualising the network environment and how it interacted with the surrounding competing wireless environments. This testing technique was also effective in detecting the Access Points (AP's) transmitting within the test area and could ascertain their MAC addresses, what channel they were transmitting on and the security encryption standards they were using. With this information a complete map of the test area was made and details of those Access Points could be seen. With this information an attacker could locate vulnerable devices to attack such as the AP listed as NetGear_Ali which is broadcasting without any security encryption and is therefore open to anyone within range.

4.3 Network Device Vulnerability Assessment

Due to the limitations associated with the scans conducted during the primary testing plan described which is considered as a primary scanning technique only for wireless network device detection. The spectrum analysis and site survey tests needed a secondary set of scans at the network level to determine the extent of potential device vulnerability. These tests were accomplished by scanning the test network with WiFi Network Analyser, Net Scan, NetGear Genie, Bluetooth Scanner and finally Nmap which are all network scanning tools. These results are summarised in table 9. These show the effectiveness of the scanning tool when detecting vulnerabilities associated with the test devices used in this research.

Table 8. Device Vulnerability Summary

Nmap	Nmap was able to scan all devices on the network and test them against several vast databases of known device security vulnerabilities. This scanning tool was effective in discovering device IP addresses, MAC addresses, OS information, and Vendor information such as type of device as well as open ports and the services and firmware that run on them that could be exploited.
WiFi Network Analyser	This scanning tool was only partially effective in finding devices transmitting over the network. It could only find certain Wi-Fi devices and could not find the Bluetooth devices on the network. This scanning tool was also completely ineffective in finding devices vulnerabilities.

Net Scan	This scanning tool was effective in finding Wi-Fi devices transmitting over the network but ineffective at finding Bluetooth devices. This scanning tool was also effective in detecting device IP addresses, MAC addresses, Vendor information and open ports that could be exploited.
NetGear Genie	This scanning tool was able to find all devices connected to the network apart from the Bluetooth devices and was able to discover limited information on the devices such as MAC addresses, OS information and IP addresses.
Bluetooth Scanner	This scanning tool was disappointing as it could only find Bluetooth devices transmitting on the network if they were in discoverable mode. This is problematic as most Bluetooth devices are set as a default to non-discoverable rendering them invisible to this scan.

From the scans, it was found that WiFi Network Analyser and Bluetooth Scanner were completely ineffective in discovering device vulnerabilities and were also limited in what devices they could discover. Both Nmap and Net Scan are effective scanning tools that could be used to interrogate a network to discover device vulnerability. These scanning tools were able to discover detailed information on the test devices such as device type, services running on open ports and other information that could be used by an attacker to infiltrate the home IoT network.

Table 9. Device Discovery Results from Different Scanning Tools

Device Name	Spectrum Analyser **(In Isolation)**	Nmap	WiFi NW Analyser	Net Scan	NetGear Genie	Bluetooth Scanner	Ekahau Site Survey Planner
NetGear R6300 (Router)	Y	Y	Y	Y	Y	N	Y
Samsung Galaxy S2	Y	Y	Y	Y	Y	Y	N
Amazon Kindle Fire	Y	Y	Y	Y	Y	Y	N
Vu+ Duo	Y	Y	Y	Y	Y	N	N
Samsung Smart TV (UE46C8000)	Y	Y	Y	Y	Y	N	N
Motorola Focus66-W (Wifi Security Camera)	Y	Y	Y	Y	Y	N	N
Microsoft Wireless Laser Mouse 8000	Y	N	N	N	N	Y	N
Microsoft Wireless Keyboard 8000	Y	N	N	N	N	Y	N
Lenovo Y70 Touch	Y	Y	Y	Y	Y	Y	N
Fitbit Surge	Y	N	N	N	N	Y	N
Microsoft Surface Book	Y	Y	Y	Y	Y	Y	N
Motorola MBP33 (Baby Monitor)	Y	N	N	N	N	N	N
Pioneer MVH X580DAB	Y	N	N	N	N	Y	N
Hinari Microwave Oven (650w)	Y	N	N	N	N	N	N
Panasonic KX-TG732 1E (Cordless Phone)	Y	N	N	N	N	N	N

In table 10 we can see the effectiveness of the results of the spectrum analyser's scans when it comes to detecting devices transmitting in the IoT network environment against that of traditional scanning means. This study aimed to learn if these RF scanning techniques would aid in a layered security policy. This set of results while encouraging that the Ekahau Spectrum Analyser can find these devices within the network by their spectrum pattern this would not be a sufficient means of security and would still require traditional scanning means as shown in table 10. This scanning technique as shown in this research provides an additional means of detecting devices transmitting over the networks airwaves only. While the results summarised in Table 15 show that this scanning technique can detect devices that other traditional scanning methods might miss it is limited by its

inability to provide vulnerability assessments of these devices. This limitation would require one of the other test solutions be used to uncover whether the devices had any vulnerabilities.

The passive scanning tools used during supplementary tests included WiFi Network Analyser, Net Scan, Bluetooth Scanner and NetGear Genie. These scanners were effective in finding most of the devices. WiFi Network Analyser found basic information on the network access point and several the devices connected to the network but was unable to provide any security vulnerability information. Net Scan could find the same devices as WiFi Network Analyser but had the added functionality of being able to scan the ports in use by the devices and interface with them. NetGear Genie could detect all the devices connected to the NetGear R6300 router that was used during testing both wired and wireless device types but again was only able to provide basic information on the connected devices. Bluetooth Scanner was a very limited passive scanning application that was only able to detect Bluetooth devices that were in discoverable mode and had no capability to detect non-discoverable devices. Even with the disappointment of Bluetooth scanner over its capabilities it still could fill a gap in detecting Bluetooth devices transmitting on the network that the others were unable to detect. The aggressive active scanner utilized during testing Nmap (Network Mapper) was a significantly more comprehensive scanning tool. This scanning tool could find all the devices connected to the network access point apart from the Bluetooth devices. This scanner could obtain extremely useful reconnaissance information about the devices on the network such as operating systems used, IP address, MAC address, open ports the services that were running on them and their version numbers. This scanner was able to run a comparative check against known security vulnerabilities amassed on several security vulnerability databases against the devices connected to the network.

5. Conclusion

RF spectrum analysis is an effective way of monitoring network traffic over the air waves. We demonstrate using a spectrum analyser and Chanalyzer software to detect network devices as a way of identifying a specific device transmitting over-the-air. As the equipment is generally designed to function as a wireless interference detection tool it is particularly effective in identifying interfering signal patterns. Without a good knowledge of these patterns and how they display however one would still not able to comprehensively conclude that the signal pattern is indeed a specific device. Evidence gathered from primary testing proves that with knowledge of how signal patterns display from specific sources it is possible to detect specific devices within the network environment. The equipment is also effective in determining the source of these signals by proximity detection when signal isolation is possible. It can be concluded this form of investigation is particularly effective at detecting devices that operate at known frequencies and broadcast at significant signal strengths. Common problems in detection can arise with certain devices such as Bluetooth devices that by their very nature hop frequency at a high rate with a low power amplitude making detection using this technique more problematic but not completely ineffectual. This testing technique while not perfect is a valid security testing technique due to its ability to detect devices transmitting over the air and the Chanalyzer software's ability to monitor and record this raw data for analysis making it a crude type of Intrusion Detection System (IDS). It can also be concluded from this primary series of tests that using site survey software as described can be an effective way of visualizing how a home network exists and interacts with nature and competing wireless networks. This can aid in inventorying all the access points (AP's) transmitting in the surrounding area as well as the signal distance broadcast by the networking equipment used. This is a factor that network owners can forget and can be a security risk when network coverage extends beyond the borders of the owner domain and can be picked up by a neighbouring property.

As of now there are only a few solutions available to a home owner if they want to secure and monitor their home IoT network. This problem has arisen due to the growth IoT devices that can be found within the home network environment. These devices can be a combination of several types that communicate using different communication protocols which can impact the security of the home environment. To police these networks using standard techniques such as firewalls and IDS/IPS would be inadequate. With so many signals transmitting over network frequencies it is hard to know what exactly is transmitting. In this study we show a security monitoring technique that could help detect signals being transmitted, interference patterns or signals attributed to malicious forces that can impact the security of an IoT network. At present this service can be provided by moderately expensive commercial devices/solutions such as the Cisco Clean Air technology that integrates the access point (AP) with a spectrum analyser chip. That device is capable of discerning what the RF signals being transmitted are attributed to. Other hardware/software solutions exist that are extremely expensive and would not be a reasonable solution to the common home owner such as the Fluke WLAN Design and Analysis Suite. This combination bundles a powerful spectrum analyser with an analysis software suite capable discovering and identifying devices transmitting on your network and delivering a security audit of potential associated

vulnerabilities. Future work is planned to expand the number of IoT devices that can be investigated and to expand the study to more diverse real-world home environments over longer periods.

References

1. Miessler, D. (2014). Internet of Things State of the Union Study. San Francisco: HP Fortify on Demand.

2. Barajas, O. (2020). How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape. Available: https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/.

3. Woods, V & van der Muelen, R. (2016). Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. Available: http://www.gartner.com/newsroom/id/3185623.

4. Voas, J. (2016). NIST Special Publication 800-183 Networks of 'Things'. Gaithersburg, MD: National Institute of Standards and Technology (NIST)

5. Kovacs, E. (2017). FTC Seeks Tools for Securing Home IoT Devices. Security Week, February 2017, http://www.securityweek.com/ftc-seeks-tools-securing-home-iot-devices.

6. Li, J. (2020) Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST). Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 1-8, Vol. 4, No. 3, 1st July 2020, DOI: 10.33166/AETiC.2020.03.001

7. Paganini, P. (2020). NewWorldHackers and Anonymous behind massive DDoS attack on Dyn DNS service. Available: http://securityaffairs.co/wordpress/52583/hacking/dyn-dns-service-ddos-3.html.

8. Krebs, B. (2016). KrebsOnSecurity Hit With Record DDoS. Krebs on Security Blog, March 2016: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

9. Caltum, E and Segal, O. (2016). SSHowDowN Exploitation of IoT devices for Launching Mass-Scale Attack Campaigns. Cambridge, Massachusetts: Akamai Threat Advisory

10. Wi-Fi Alliance (2020). Who We Are - History. Wi-Fi.Org, : http://www.wi-fi.org/who-we-are/history.

11. Mehl, B. (2015). Internet Of Things Communication Protocols. GetKisi, https://blog.getkisi.com/internet-of-things-communication-protocols/.

12. Poole, I. (2020). Bluetooth Security. http://www.radio-electronics.com/info/wireless/bluetooth/security.php.

13. Kambourakis, G., Kolias, C., Stavrou, A. (2017) The mirai botnet and the iot zombie armies. MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017. pp: 56-68, Baltimore, MD, USA. ISSN: 2155-7586, DOI: 10.1109/MILCOM.2017.8170867

14. Augusto-Gonzalez, Javier, et al. "From internet of threats to internet of things: A cyber security architecture for smart homes." 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019.

15. Zhong, H, Xiao, J. (2014). Design for Integrated WiFi Defence Strategy in Mordern Enterprise Context. IEEE International Conference

16. Waliullah, M, Gan, D. (2014). Wireless LAN Security Threats & Vulnerabilities: A Literature Review. (IJACSA) International Journal of Advanced Computer Science and Applications. 5 (1), 176-183.

17. Gupta, N (2018). Inside Bluetooth Low Energy. Boston: Artech House. 1-385.

18. Dubey, V K, Vaishali, K, Behar, N, Shrivastava, M. (2015). A Review on Bluetooth Security Vulnerabilities and a Proposed Prototype Model for Enhancing Security against MITM Attack . International Journal of Research Studies in Computer Science and Engineering (IJRSCSE). 0 (0), 69-75.

19. Uher, J, Mennecke R.G, Farroha B.S. (2016). Denial of Sleep Attacks in Bluetooth Low Energy Wireless Sensor Networks. MILCOM 2016 - 2016 IEEE Military Communications Conference. 1 (1), 1231-1236.

20. Kostadinov, D. (2020). Hacking ZigBee Networks. Available: http://resources.infosecinstitute.com/hacking-zigbee-networks/. Last accessed 16th Apr 2017.

21. He, D, Zeadally, S. (2015). An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. IEEE Internet of Things Journal. 2 (1), 72-83.

22. Williamson Sr, A, Tsay, L, Kateeb, I, Burton, L. (2013). Solutions for RFID Smart Tagged Card Security Vulnerabilities. AASRI Conference on Intelligent Systems and Control. 4 (1), 282-287.

23. Grover, A & Berghel, H. (2011). A Survey of RFID Deployment and Security Issues. Journal of Information Processing Systems. 7 (4), 561-580.

24. Kavya, S, Pavithra, K, Rajaram, S, Vahini, M, Harini, N. (2014). Vulnerability Analysis and Security System For NFC-Enabled Mobile Phones. International journal of scientific & technology research. 3 (6), 207-210.

25. Alsafi, H.M.A., Basahm, S.S. (2013). A Review of Intrusion Detection System Schemes in Wireless Sensor Network . Journal of Emerging Trends in Computing and Information Sciences. 4 (9), 688-697.

26. Newlin, M. (2019). KeySniffer Technical Details. Keysniffer.net, march 2019. https://www.keysniffer.net/technical-details/

27. Gallagher, S. (2015). "Funtenna" software hack turns a laser printer into a covert radio. Ars Technica, August 2015, https://arstechnica.com/security/2015/08/funtenna-software-hack-turns-a-laser-printer-into-a-covert-radio/.

28. Ali, K, Liu, A, Wang, W, Shahzad, M. (2017). Keystroke Recognition Using WiFi Signals. IEEE Journal on Selected Areas in Communications. 99 (1), 90-102.

29. Griffor, E., Greer, C., Wollman, D., Burns, M. (2017) Framework for Cyber-Physical Systems: Volume 1, Overview, DOI: 10.6028/NIST.SP.1500-201

30. Tian, D., Scaife, N., Kumar, D., Bailey, M., Bates, A., and Butler, K. (2018) "SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions 1 through C," in Proceedings of the 39th IEEE Symposium on Security and Privacy (Oakland), San Francisco, CA, USA, May 21- 23, 2018, 2018.

31. Scarfone, K., Mell, P. (2012) SP 800-94 Rev. 1(Draft) Guide to Intrusion Detection and Prevention Systems (IDPS), July 2012 https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft

32. GSMA (2016) IoT Security Guidelines for Network Operators v1.0, GSMA, https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.14-v1.0.pdf

33. PCI (2019) PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.1, https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf